RSAC 2025 Conference

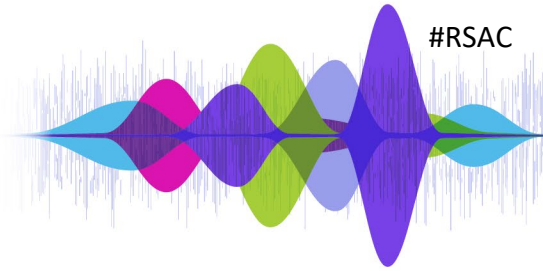
Many Voices.
One Community.

SESSION ID: HT-T02

Blowing Up Gas Stations for Fun and Profit

Pedro Umbelino

Principal Research Scientist
Bitsight
https://www.linkedin.com/in/pedroumbelino



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Agenda

- ATGs
- Device prevalence
- Legacy protocol issues
- Newer device issues
- Disclosure process
- The quest of physical damage
- Conclusions

Automated Tank Gauges

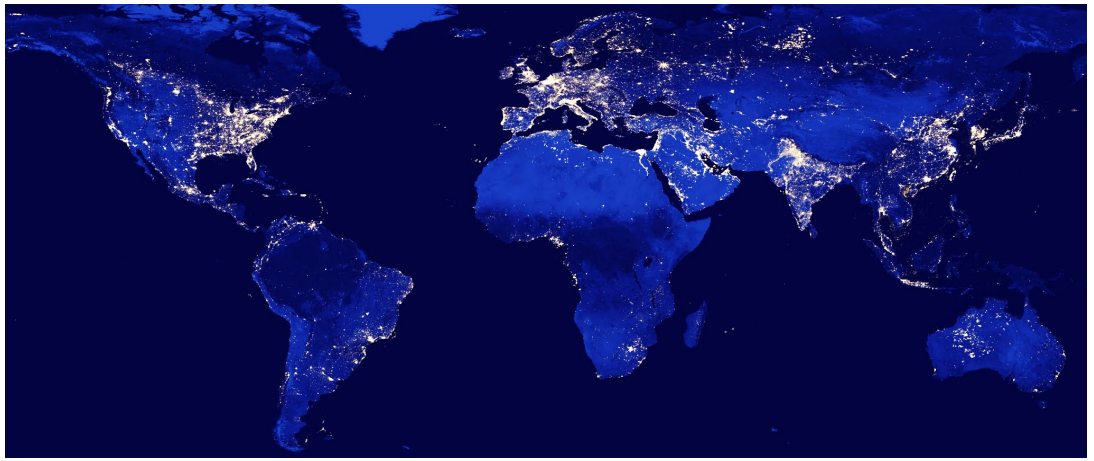
What is an Automated Tank Gauge (ATG) system?

- Fuel tank Industrial Control System (ICS)
- Leak monitoring and alarms
- Inventory management
- Environmental compliance
- Several use cases, besides gas stations

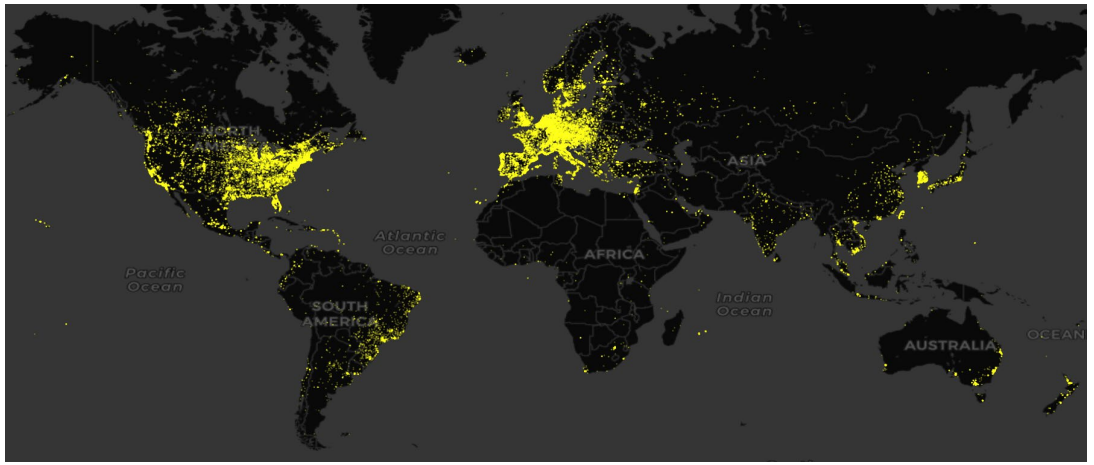
Automated Tank Gauges

Why Are We Researching ATGs?

- Critical infrastructure sectors is heavily reliant on Industrial Control Systems (ICS)
- That led to the construction of our ICS physical laboratory
- We are conducting multiple research initiatives on ICS protocols



(NASA: The World at Night)

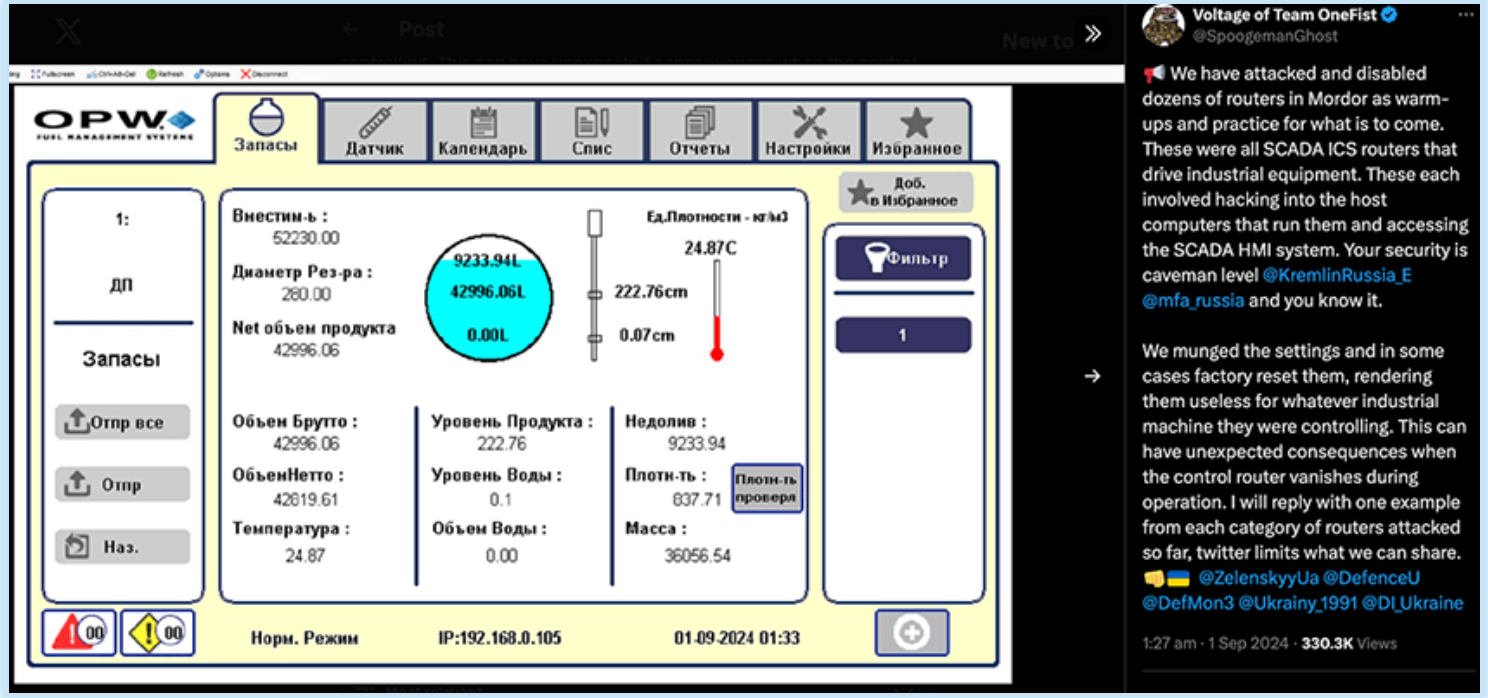


(Bitsight: ICS/OT Top Protocol Exposures)

Automated Tank Gauges

Why Are We Researching ATGs?

- This research is not about a theoretical threat.
- ICS/OT systems are currently being targeted in warfare scenarios.

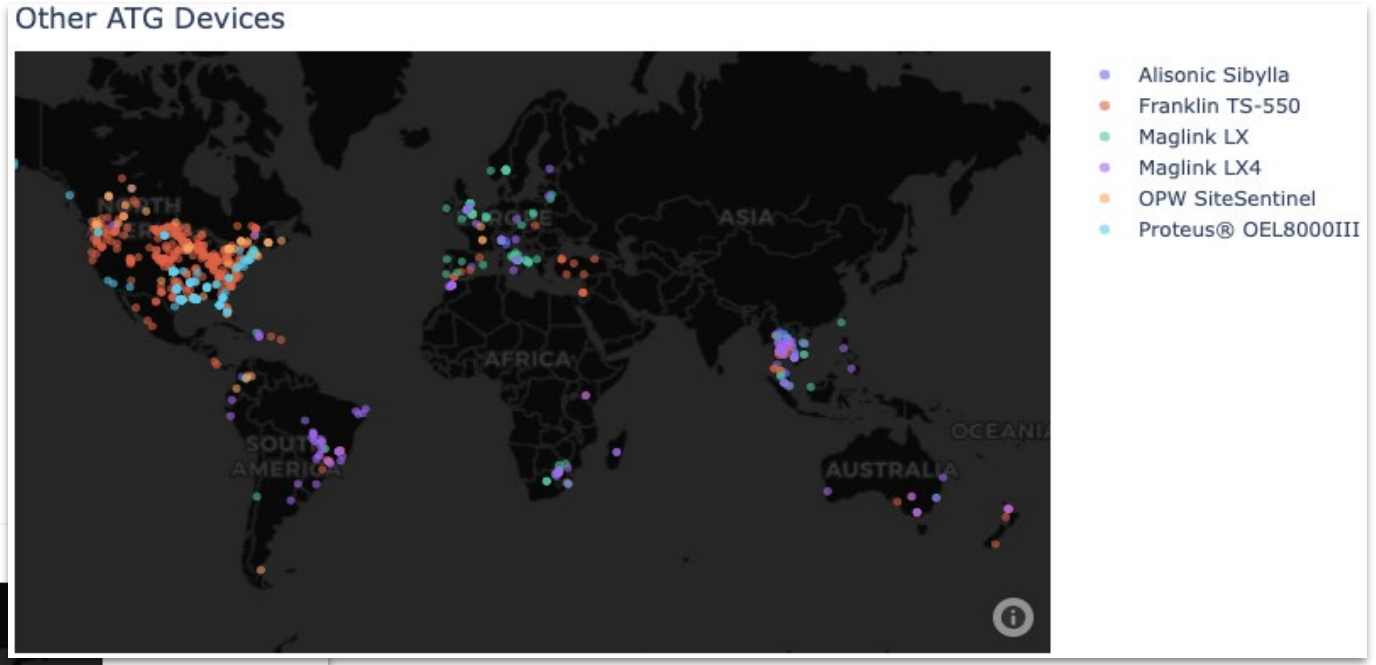


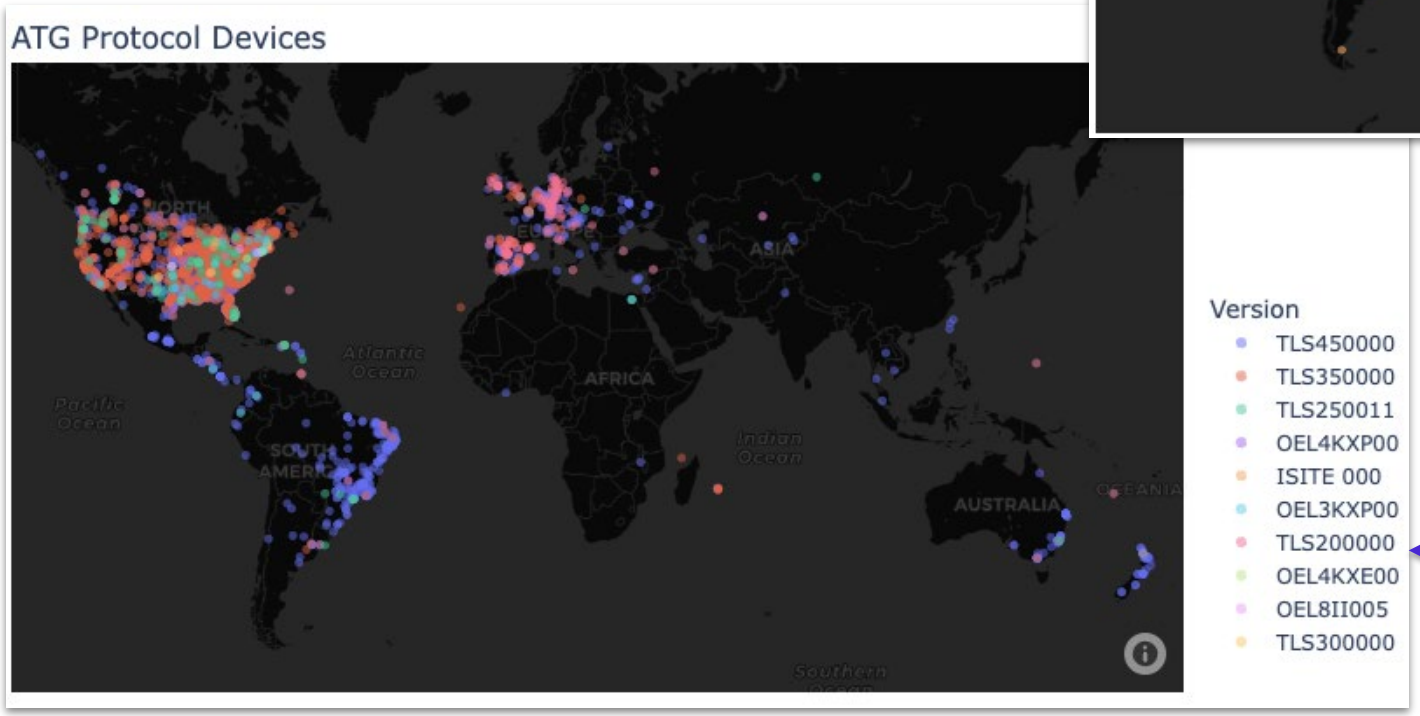
(X: Voltage of Team OneFist)

ATG Prevalence

ATG Protocol vs. newer ATG Devices

- Different devices, protocols, interfaces, vulnerable just the same





- Usually no ATG protocol, mostly web interface (>1200 devices)
- ATG protocol (> 9000 as of 2025)

RSAC 2025 Conference

ATG Device Types

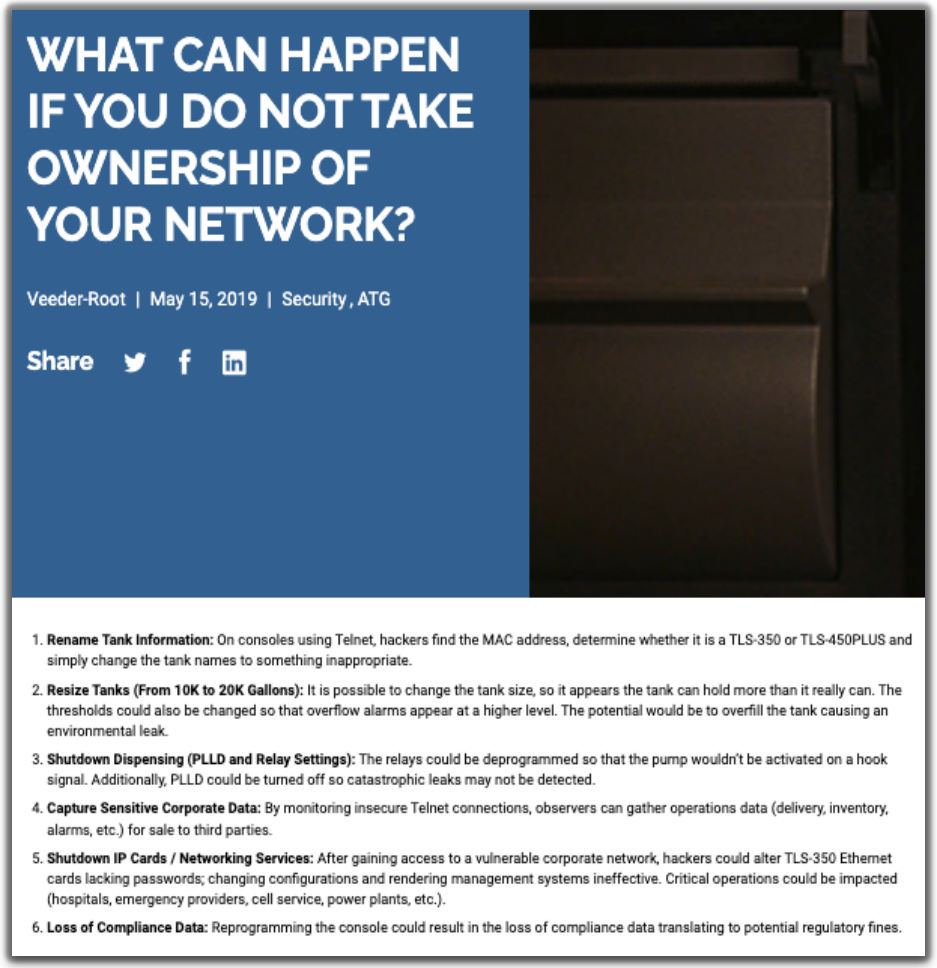
the legacy and the new

Many Voices.
One Community.

ATG Protocol

Past security research

- ATG protocol security issues were back in 2015
- Protocol open by default.
- Recognized exploitation impact include:
  - Resizing tanks
  - Shutdown dispensing
  - Shutdown the network
  - Loss of compliance data



WHAT CAN HAPPEN IF YOU DO NOT TAKE OWNERSHIP OF YOUR NETWORK?

Veeder-Root | May 15, 2019 | Security, ATG

Share

1. **Rename Tank Information:** On consoles using Telnet, hackers find the MAC address, determine whether it is a TLS-350 or TLS-450PLUS and simply change the tank names to something inappropriate.
2. **Resize Tanks (From 10K to 20K Gallons):** It is possible to change the tank size, so it appears the tank can hold more than it really can. The thresholds could also be changed so that overflow alarms appear at a higher level. The potential would be to overfill the tank causing an environmental leak.
3. **Shutdown Dispensing (PLLD and Relay Settings):** The relays could be deprogrammed so that the pump wouldn't be activated on a hook signal. Additionally, PLLD could be turned off so catastrophic leaks may not be detected.
4. **Capture Sensitive Corporate Data:** By monitoring insecure Telnet connections, observers can gather operations data (delivery, inventory, alarms, etc.) for sale to third parties.
5. **Shutdown IP Cards / Networking Services:** After gaining access to a vulnerable corporate network, hackers could alter TLS-350 Ethernet cards lacking passwords; changing configurations and rendering management systems ineffective. Critical operations could be impacted (hospitals, emergency providers, cell service, power plants, etc.).
6. **Loss of Compliance Data:** Reprogramming the console could result in the loss of compliance data translating to potential regulatory fines.

ATG Protocol

Recent security research

- **2015** - 5,800 ATGs exposed (**Rapid7**)
- **2024** - 6,542 ATGs, excluding GasPots, exposed (**Bitsight**)
  - *What about devices with the security code enabled?*

The RS-232 security code is an optional six-digit code used to limit external serial access to the system for security purposes. It can be set to any unique set of characters using either the front panel switches or the external communication interface setup commands. The system will not respond to a command without the proper security code, if the DIP switch is set to enable RS-232 security.

ATG Protocol

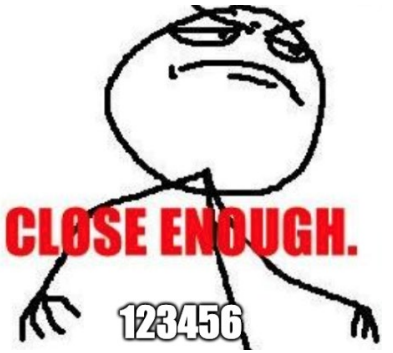
Fingerprinting security code protected devices

- Protected device do not reply at all
- Challenge to fingerprint
- Statistics to the rescue
  - 123456 is the single most used 6-digit password (**wow!!**)
  - 57 devices found
  - Hence ~570ish code protected devices out there?

Table 6: Top ten 6-digit PINs in each PIN dataset

Rank	Dodonew		CSDN		Rockyou		Yahoo	
1	123456	17.05%	123456	10.73%	123456	11.69%	123456	11.05%
2	111111	2.15%	123123	0.97%	654321	0.56%	111111	0.92%
3	123123	2.01%	111111	0.68%	111111	0.51%	123123	0.63%
4	000000	1.29%	123321	0.53%	000000	0.49%	654321	0.54%
5	**321654**	1.00%	000000	0.47%	123123	0.40%	000000	0.41%
6	123321	0.55%	654321	0.27%	666666	0.29%	**030379**	0.39%
7	**520131**	0.53%	112233	0.24%	121212	0.21%	666666	0.31%
8	**520520**	0.44%	**123654**	0.21%	112233	0.21%	123321	0.30%
9	112233	0.30%	520520	0.21%	**789456**	0.21%	121212	0.29%
10	**147258**	0.30%	666666	0.20%	**159753**	0.20%	**101471**	0.28%
Total	736,843	25.62%	117,516	14.51%	407,429	14.77%	3,178	15.12%

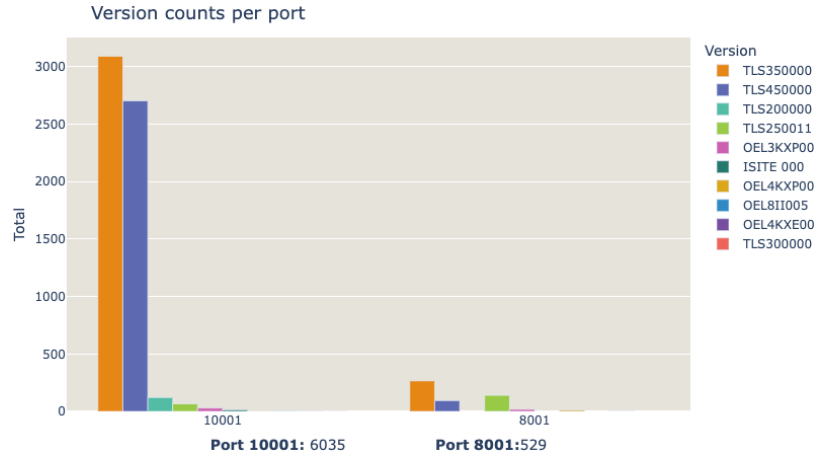
Understanding Human-Chosen PINs: Characteristics, Distribution and Security (Ding Wang, Qianchen Gu, Xinyi Huang, Ping Wang)

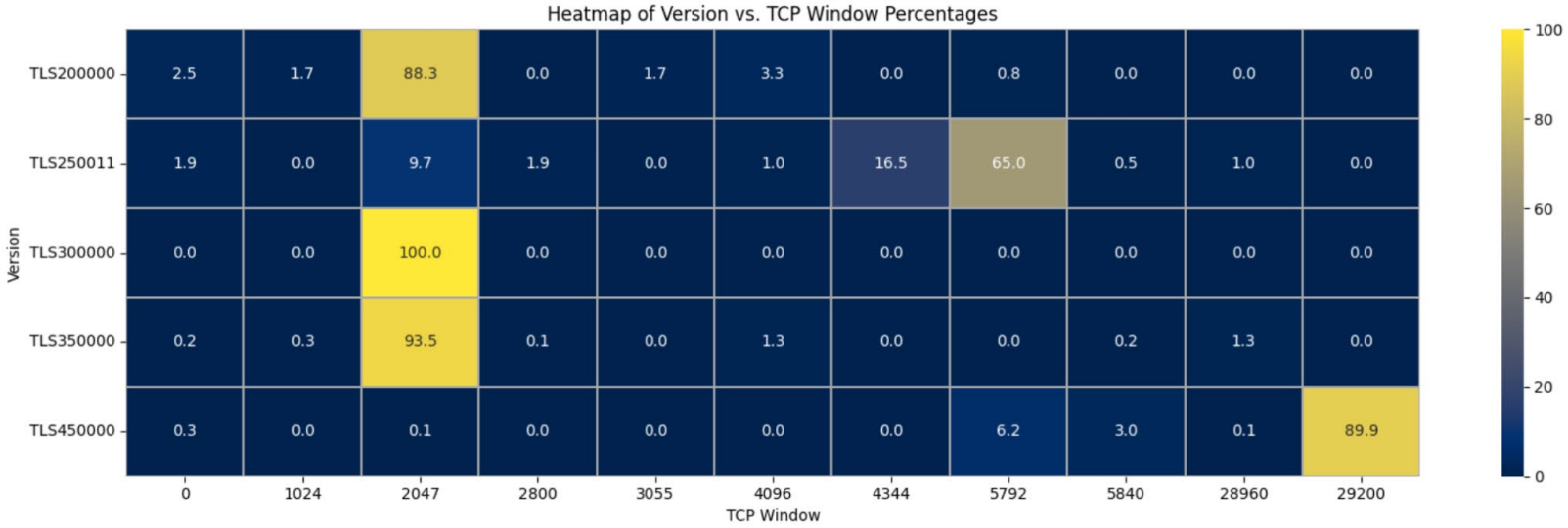


ATG Protocol

Fingerprinting all devices

- Avoid GasPots
- Check nonstandard ports
- Serial(ish) protocol is running underneath
- Consider TCP/IP quirks





Newer ATG devices

ATG ecosystem is diverse in vendors and devices

- Older devices use the ATG protocol
- Newer devices can support the ATG protocol
- Newer devices also rely on web interfaces to setup, monitor and control
- This leads to an increased attack surface

Newer ATG devices

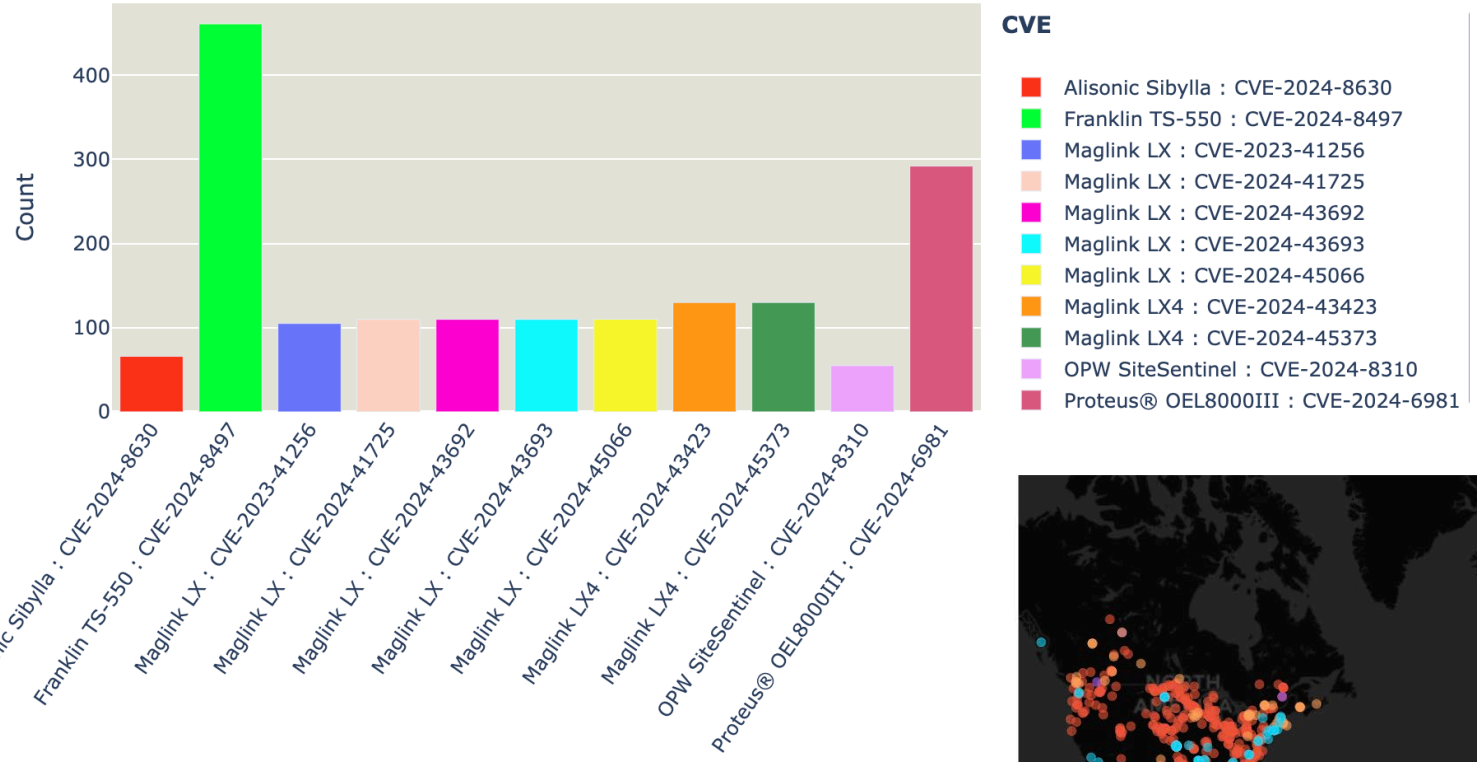
Multiple critical vulnerabilities across 6 ATG systems from 5 vendors.

- *Ten 0-day vulnerabilities found*
- *Reflection of the overall security status in the ICS sector in general*
- *The majority of those obey the criteria of the Unforgivable Vulnerabilities**

PRODUCT	VULNERABILITY TYPE	CVE	CVSS 3.1
Maglink LX	OS Command Injection	CVE-2024-45066	10.0
Maglink LX	OS Command Injection	CVE-2024-43693	10.0
Maglink LX4	Hardcoded credentials	CVE-2024-43423	9.8
OPW SiteSentinel	Authentication Bypass	CVE-2024-8310	9.8
Proteus® OEL8000	Authentication Bypass	CVE-2024-6981	9.8
Maglink LX	Authentication Bypass	CVE-2024-43692	9.8
Alisonic Sibylla	SQL Injection	CVE-2024-8630	9.4
Maglink LX	XSS	CVE-2024-41725	8.8
Maglink LX4	Privilege Escalation	CVE-2024-45373	8.8
Franklin TS-550	Arbitrary File Read	CVE-2024-8497	7.5

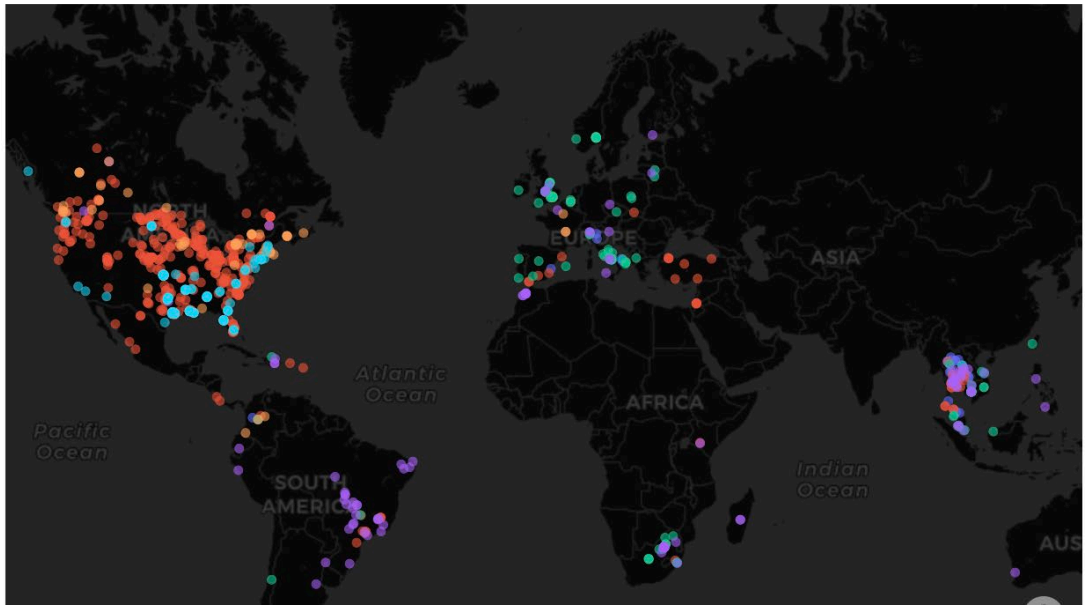
* https://cwe.mitre.org/documents/unforgivable_vulns/unforgivable.pdf

Newer ATG devices



Geographic bias

- *These models seem to have a heavy deployment on the US, Brasil and Thailand*
- *Some models seemed almost exclusively European*



RSAC 2025 Conference

About Those Vulnerabilities

and how we disclosed them

Many Voices.
One Community.

Newer ATG devices

Vulnerability type quick break down

- ***OS Command Injection***
  - *Details left as an exercise to the reader*
  - *Classic injection on network diagnostics*

PRODUCT	VULNERABILITY TYPE	CVE	CVSS 3.1
Maglink LX	OS Command Injection	CVE-2024-45066	10.0
Maglink LX	OS Command Injection	CVE-2024-43693	10.0

Newer ATG devices

Vulnerability type quick break down

- ***Hardcoded credentials***
  - *Details left as an exercise to the reader*
  - *Undeletable super admins*
  - *Passwords were just too 31337*

PRODUCT	VULNERABILITY TYPE	CVE	CVSS 3.1
Maglink LX4	Hardcoded credentials	CVE-2024-43423	9.8

Newer ATG devices

Vulnerability type quick break down

- ***Authentication bypass***
  - *Details left as an exercise to the reader*
  - *Authentication logic client side a.k.a. the browser decides if you are authenticated. What? What?...*

PRODUCT	VULNERABILITY TYPE	CVE	CVSS 3.1
OPW SiteSentinel	Authentication Bypass	CVE-2024-8310	9.8
Proteus® OEL8000	Authentication Bypass	CVE-2024-6981	9.8
Maglink LX	Authentication Bypass	CVE-2024-43692	9.8

Newer ATG devices

Vulnerability type quick break down

- ***SQL Injection***
  - *Details left as an exercise to the reader*
  - *Aided by full error messages*

PRODUCT	VULNERABILITY TYPE	CVE	CVSS 3.1
Alisonic Sibylla	SQL Injection	CVE-2024-8630	9.4

Newer ATG devices

Vulnerability type quick break down

- ***Cross Site Scripting***
  - *Details left as an exercise to the reader*

PRODUCT	VULNERABILITY TYPE	CVE	CVSS 3.1
Maglink LX	XSS	CVE-2024-41725	8.8

Newer ATG devices

Vulnerability type quick break down

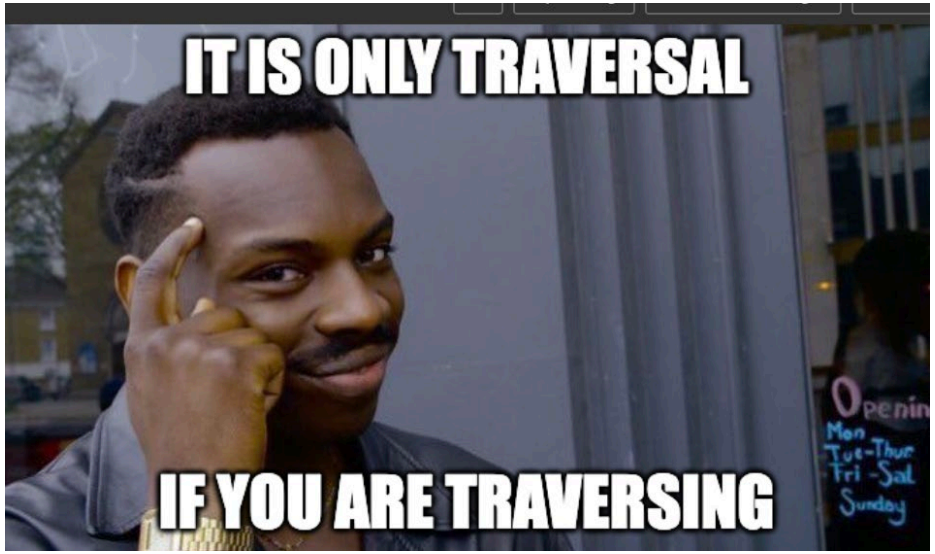
- ***Privilege escalation***
  - *Details left as an exercise to the reader*

PRODUCT	VULNERABILITY TYPE	CVE	CVSS 3.1
[redacted]			
Maglink LX4	Privilege Escalation	CVE-2024-45373	8.8
[redacted]			

Newer ATG devices

Vulnerability type quick break down

- ***Direct File Access***
  - *Details left as an exercise to the reader*
  - *Direct file access*



PRODUCT	VULNERABILITY TYPE	CVE	CVSS 3.1
Franklin TS-550	Arbitrary File Read	CVE-2024-8497	7.5

Newer ATG devices

Criteria for an “Unforgivable Vulnerability”

1. Precedence
2. Documentation
3. Obviousness
4. Attack Simplicity
5. Found in Five

On responsible disclosure

Coordinated responsible disclosure challenge

- Multiple critical vulnerabilities across 6 ATG systems.
- Vulnerabilities reported on 21/03/2024
- Joint work with DHS/CISA and the vendors in a coordinated disclosure effort
- The vulnerabilities became public on the 24/09/2024

Live demo! (just kidding, it is a video)

RSAC 2025 Conference

On The Challenges Of Blowing Things Up

Just don’t! Seriously.

Many Voices.
One Community.

Quest for physical damage

Ideas and techniques

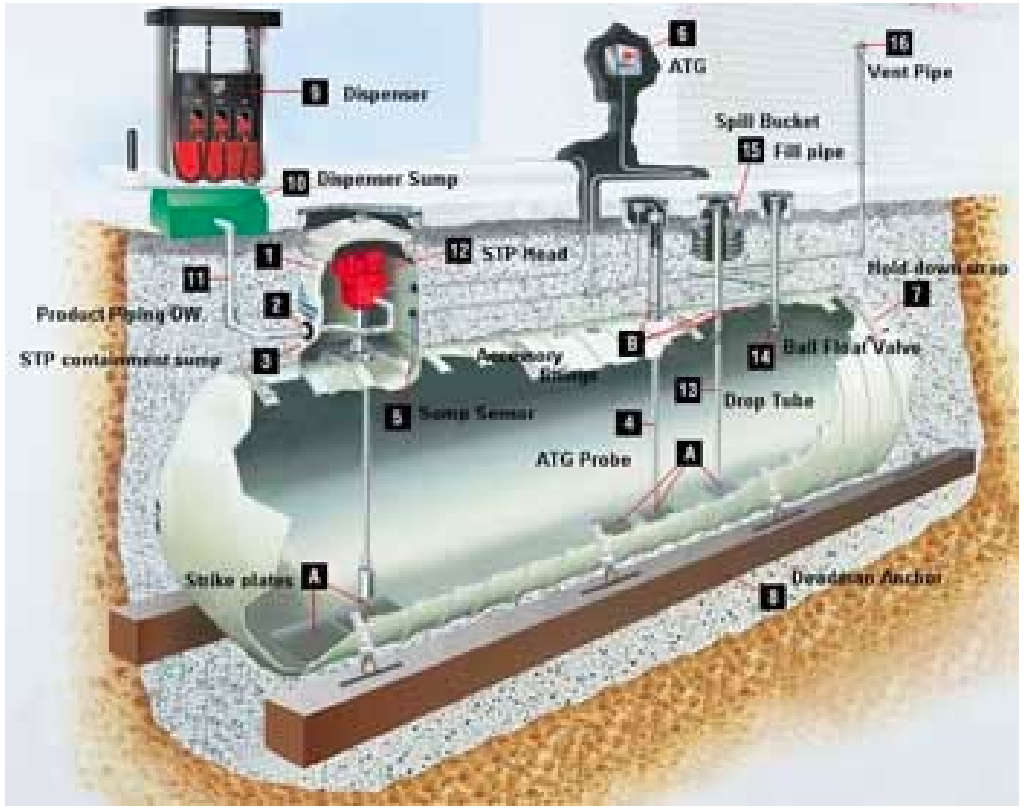
- **Why**
  - It is truly the most responsible thing to do
  - Because I just have to, it's a condition I suffer from…
- **How**
  - Sensors and actuators
  - Living off the land
  - Legacy protocol strikes back

Quest for physical damage

Ideas and techniques brainstorm

- DoS is trivial…
- Flashing / corrupting the OS is easy…
- Doesn't make a gas station go **boom**!

- What might?
  - Aiming for the sensors
  - Aiming for the actuators



Quest for physical damage

Aiming for the sensors

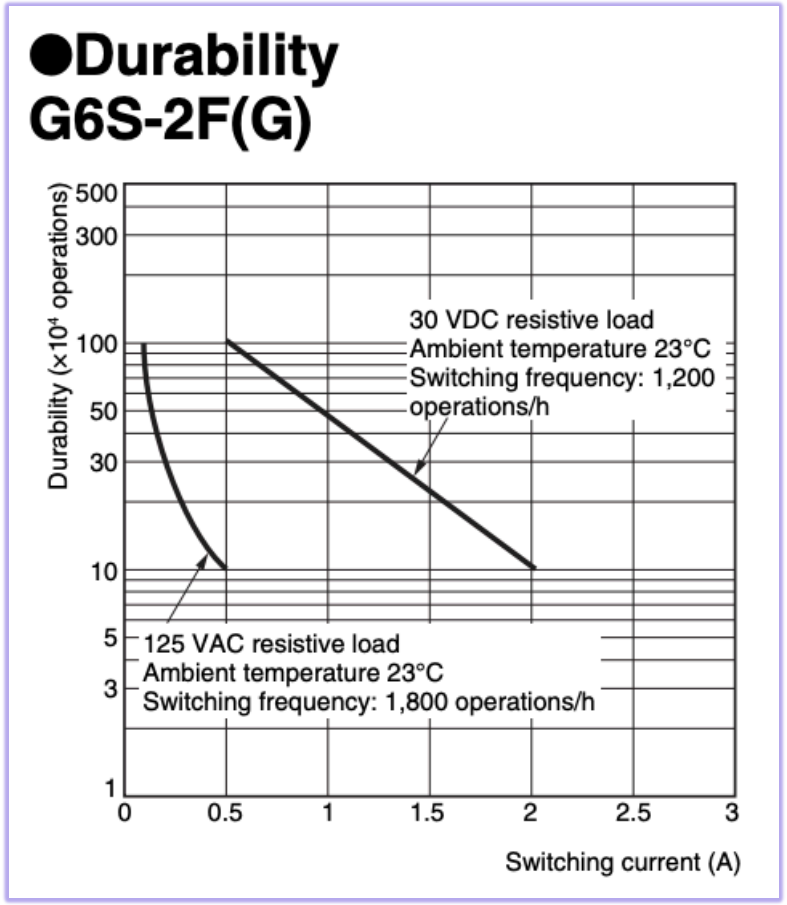
- Fuel / water level sensor
- Resizing tank geometry
  - Reduces reaction time for refueling technician
- Disabling leak detection, environmental impact
- Simulating problems at scale can have even wider impact and a trickle-down effect

Quest for physical damage

Aiming for the actuators

- ATGs not only read sensors but control external hardware as well
- Internal and external relay board

- Relay abuse seemed the most obvious attack



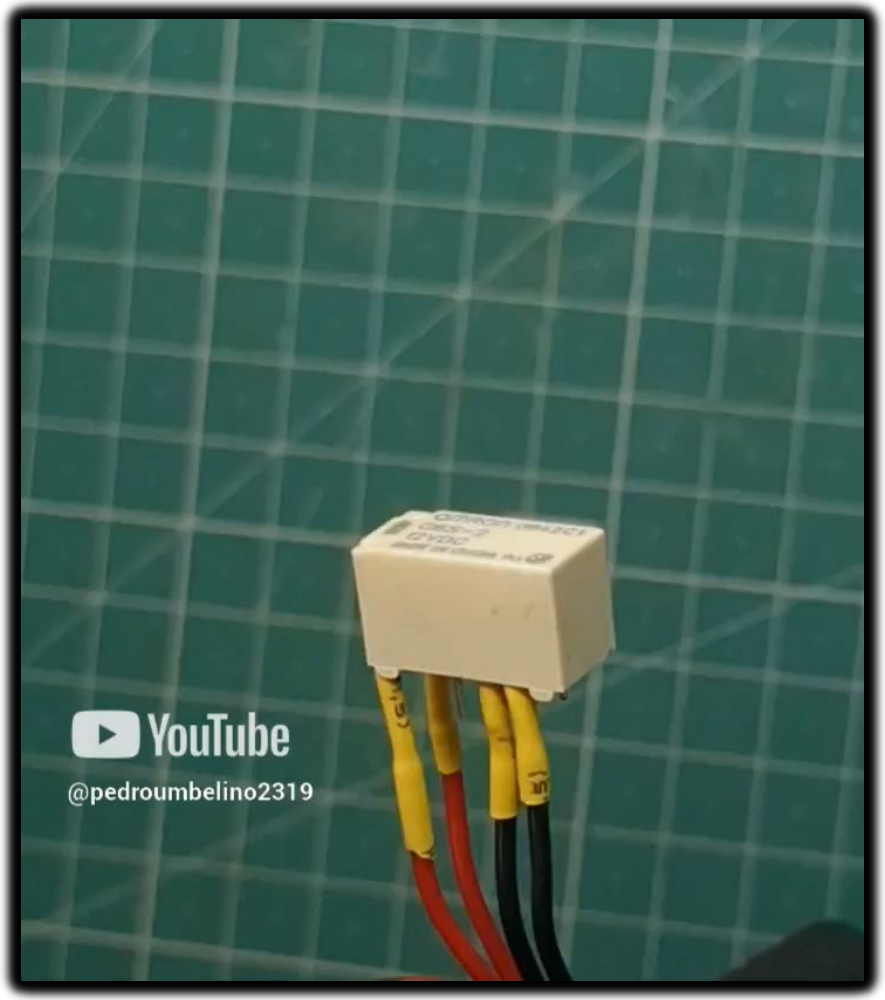
Quest for physical damage

Aiming for the actuators

How to abuse relays

- Living of the land
  - Example Maglink LX4 (i2c tools)
  - `root@imx6ul-var-dart:~# while true; do i2cset -y 0 0x21 0x14 0x01; i2cset -y 0 0x21 0x14 0x00; done`

- Your mileage may vary, depending on the hardware, but ATGs share many features.
  - `root@XXXX:~# /usr/local/bin/pmdevctl /dev/pmMicro 3`
  - `root@YYYY:~# jpeg2fb rickroll.jpg`



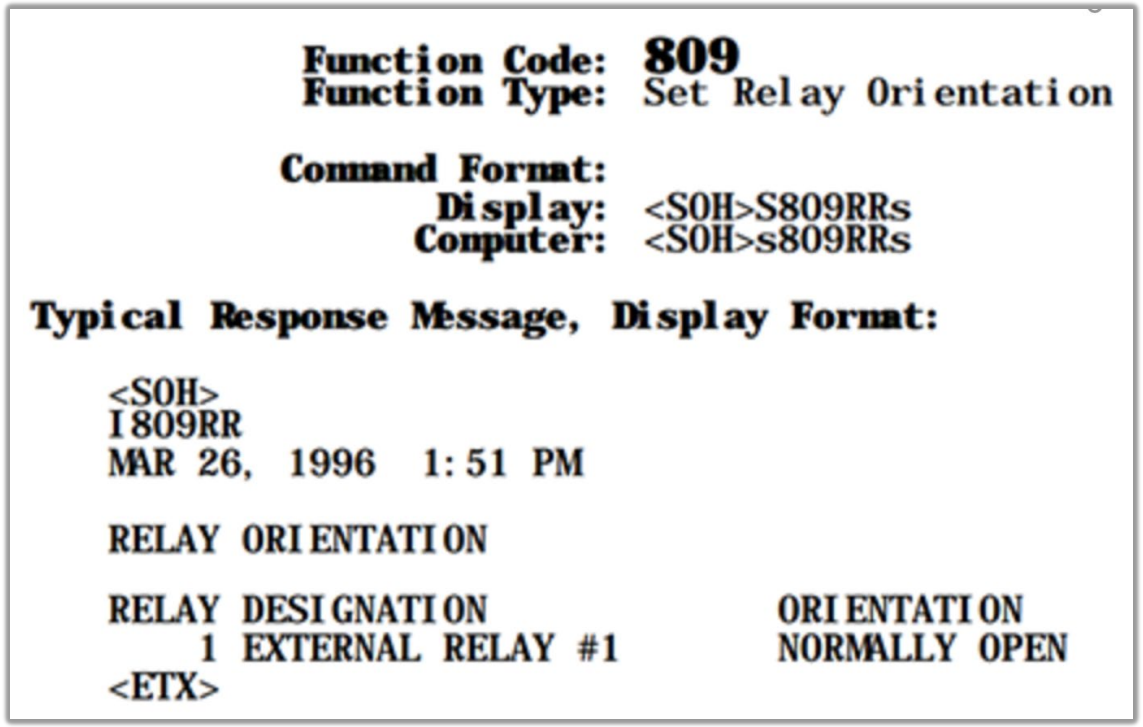
Quest for physical damage

Aiming for the actuators

How to abuse relays

- What about the old protocol?
- In short, yes, albeit it will be slower.

- **<pseudo script>:**
- **~#** `print "<SOH>S809011"| nc x.x.x.x pppp`
  - `sleep 0.1`
  - `print "<SOH>S809012"| nc x.x.x.x pppp`
  - `sleep 0.1`



Function Code: **809**
Function Type: Set Relay Orientation

Command Format:
Display: <SOH>S809RRs
Computer: <SOH>s809RRs

Typical Response Message, Display Format:

<SOH>
I809RR
MAR 26, 1996 1:51 PM

RELAY ORIENTATION

RELAY DESIGNATION	ORIENTATION
1 EXTERNAL RELAY #1	NORMALLY OPEN

<ETX>

Quest for physical damage

SUMMARY

- Is physical damage possible? **Yes**
- **Directly**
  - Attacking the relays
  - Attacking the peripherals connected to the relays
- **Indirectly (depending on external factors)**
  - Changing with tank geometry
  - Changing tank fuel information

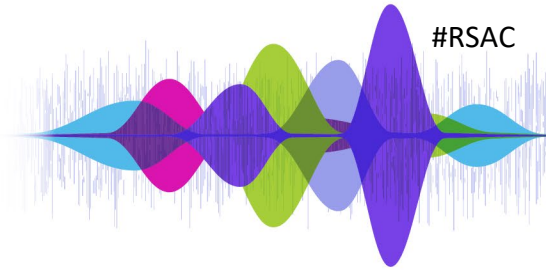
RSAC 2025 Conference

Conclusions

Wrapping it all up

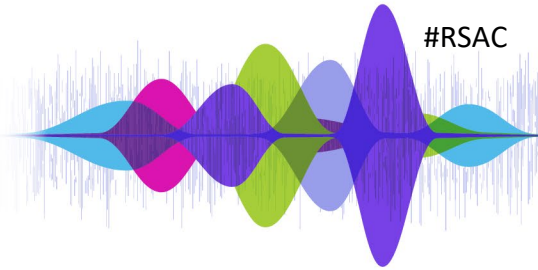
Many Voices.
One Community.

CONCLUSIONS



- **ATGs are usually part of critical infrastructure (gas stations, hospitals, power grid, telcos, military)**
- There are more ATG systems exposed now than reported 10 years ago
- **New ATGs have an increased attack surface and can introduce ‘modern’ vulnerabilities** **(there are commas on ‘modern’, in case you missed it)**
- There seem to be a lack of attention/investment in the security of these systems, judging by the types of vulnerabilities found
- **Physical damage is proven to be possible**
- Not only older ATGs are vulnerable, but newer models are too
- **ATG systems are actively being targeted by attackers**

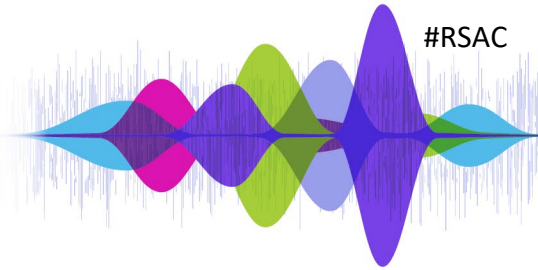
Apply What You Have Learned Today



- **Next week you should:**
  - Identify any ATG device in your organization. Understand if they have communications or administration ports directly exposed to the internet.
- **In the first three months following this presentation you should:**
  - Remove the direct exposure by putting the ATGs behind a firewall/VPN
  - If not possible, block all traffic and create specific IP allow lists
- **Within six months you should:**
  - Reassess the ATG solution deployed. Removing exposure is a temporary mitigation. Can your solution be upgraded or does it need to be replaced?

How can you drive change?

(even if you don't own a gas station)



- Are you…
  - A Cybersecurity professional?
  - A System Integrator / Certified Installer?
  - A Manufacturer?
  - A Government Policymaker?

- You too can drive change!

RSAC 2025 Conference

Many Voices.
One Community.

Thank you!
(Q&A)

For more information:

https://www.bitsight.com/blog/critical-vulnerabilities-discovered-automated-tank-gauge-systems